UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/752,385	01/06/2004	Hashem M. Ebrahimi	1565.066US1	6809

21186 7590 03/17/2011

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
LE, CANH	

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
03/17/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@slwip.com
request@slwip.com

Office Action Summary	Application No.	Applicant(s)	
	10/752,385	EBRAHIMI ET AL.	
	Examiner	Art Unit	
	CANH LE	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 July 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,6,8,10 and 12-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,6,8,10 and 12-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 07/30/2010 has been entered.

This Office Action is in response to the application 10/752385 filed on 07/30/2010.

Claims 3-5, 7, 9, 11, and 16-30 have been cancelled.

Claims 1 and 8 have been amended.

Claims 1-2, 6, 8, 10, and 12-15 have been examined and are pending.

This Action is made Non-FINAL.

Response to Arguments

Applicant's arguments, see page 6, filed 07/30/2010, with respect to the 35 U.S.C. § 112, 2nd rejection of claims 8 have been fully considered. The 35 U.S.C. §112, 2nd rejection of claim 8 has been withdrawn.

The Applicant's arguments with respect to claims 1-2, 6, 8, 10, and 12-15 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2, 6, 8, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Number 6,081,900 (hereinafter **Subramaniam**) in view of US Patent Application Publication US 2003/0131259 A1 (hereinafter **Barton**) further in view US Patent Application Publication 2003/0061387 A1 (hereinafter **Brown**).

As per claim 1:

Subramaniam teaches a method to manage secure communications implemented in a computer-readable medium and to execute on a proxy server, the method, comprising:

(a) establishing, by the proxy server, a secure session on a secure site with an external client that communicates from an insecure site **[Subramaniam : Col. 1, line 25 to Col. 2, line 25; Col. 3 lines 35-50; Col. 3, line 66 to Col. 4 line 17]**;

(b) detecting, by the proxy server, access attempts during the secure session directed to insecure transactions, the insecure transactions identified as links to a site **[Subramaniam : Col. 1, line 25 to Col. 2, line 25; Col. 6, lines 40-60; By checking the IP address which the request was made, the target server 104 determines that the request came from outside the security parameter 102. The target server 104 check user permission against access control list**

associated with the data"; fig. 1, Border server 106 includes URL transformer 108 and cache(s) 110; fig. 3; Border server 106; Col. 9, lines 32-43; "The possibly repeated acts within the transmitting step 128 involve sending one or more Web pages, files, or other pieces of non-secure data 130 from the target server 104 to the border server 106. The data 130 is non-secure in that it includes hypertext links, URLs, or other references which, if presented by the external client 112 to the secure network 100, ...which contain URLs specifying "http://" rather than "https://" in reference to data stored on the target server 104 are examples of non-secure data 130"; Col. 10, lines 10-19] [[external (external site) to, not controlled by, and not recognized by the secure site, and the access attempts are directed to the insecure transactions having references to resources of the external site]]; and

(c) transparently managing, by the proxy server, the access attempts by pre-acquiring content from the external site by accessing the links on behalf of the external client to pre-acquire the content and by scanning and inspecting the content within the secure site before determining whether the content should be made available to the external client during the secure session **[Subramaniam : Col. 1, line 25 to Col. 2, line 25 Col. 6, lines 40-60; The target server 104 check user permission against access control list associated with the data, or take other steps to make sure the requesting user is entitled to access the request data before providing data"; fig. 1, Border server 106 includes URL transformer 108 and cache(s) 110; fig. 3; Border server 106; Col. 9, lines 32-43; "The possibly repeated acts within the transmitting step 128 involve sending one or more Web pages, files, or other pieces of non-secure data 130 from the target server 104 to the border server 106. The data 130 is non-secure in that it includes hypertext links, URLs, or other references which, if**

presented by the external client 112 to the secure network 100, ….which contain URLs specifying "http://" rather than "https://" in reference to data stored on the target server 104 are examples of non-secure data 130"; Col. 10, lines 10-19; Col. 5; lines 25-27; "The secure network 100 includes one or more file or object or Web servers such as target server 104"; figs. 1, 3; The target server 104 is in the secure network 100; Col. 10, lines 59-66; "The target server 104 can then transform any non-secure data 130 to the border server 106 for subsequent transmission to the external client 112."];

Subramaniam does not explicit disclose wherein "the border server is external from the secure site, and at least one access attempt associated with at least one piece of the content that is scanned identifies a true insecure reference by determining that the true insecure reference is a particular reference that has been determined by the method to have had the piece of the content or metadata of the true insecure reference tampered with, and the true insecure reference is entirely removed from the content before the content is supplied to the external client and an event is reported as a custom warning inserted into the content supplied to the external client, the event identifies for the external client within the content that the true insecure reference was removed before being provided to the external client."

It would have been obvious to one of ordinary skill in the art at the time the invention was made to move the border server to an site external from the secure location, since it has been held that it requires routine skill in the art to rearrange the location of the border server because it would not have modified the operation of the device **[See MPEP 2144.04; see also In re Japikse, 181 F.2d 1019, 86 USPQ 70 (CCPA 1950)].**

Barton discloses transferring data via a secure network connection, wherein at least one access attempt associated with at least one piece of the content that is scanned identifies a true insecure reference by determining that the true insecure reference is a particular reference that has been determined by the method to have had the piece of the content or metadata of the true insecure reference tampered with **[Barton: par. [0012]; scanning code operable to scan said data at said proxy computer for illegal content (i.e. a true insecure reference); See also par. [0014], [0018]; par. [0033]; if illegal content is found (i.e. a true insecure reference has been tampered), then this trigger an appropriate action; fig. 4, par. [0039].**

Barton further disclose a https proxy computer scanning for illegal content and triggering an appropriate action such as sending a warning webpage to client or issue of an alert to a network administrator **[Barton: figs 4-5; par. [0033], [0039], [0040]].**

Therefore, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Barton with the teaching of Subramaniam to ensure that a transferring data does not contain any illegal content by scanning for illegal content before data is delivered to a client **[Barton: par. [0014]].**

Subramaniam and Barton do not explicitly disclose "the true insecure reference is entirely removed from the content before the content is supplied to the external client and an event identifies for external client within a content that the true insecure reference was removed before being provided to the external client, the event identifies for the external client within the content that the true insecure reference was removed before being provided to the external client" Instead, Barton disclose a https proxy computer scanning for illegal content and

triggering an appropriate action such as sending a warning webpage to client or issue of an alert to a network administrator.

However, in the same field of art. Brown teaches system and method for transcoding support of Web content over secure connection. In at least one of embodiment, Brown teaches step of executing an URL request with a modified request header, removing a set-cookie directive from header, and sending modified http response to a client **[Brown: fig. 4, par. [0032-0041]; modified a request header' removed a set-cookie directive from http response. Set-cookie directives are not sent to client; Send modified http response to client].**

Therefore, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Brown with the teaching of Subramaniam and Barton invention, by implementing *"the true insecure reference is entirely* removed from the content before the content is supplied to the external client and an event is reported as a custom warning inserted into the content supplied to the external client, the event identifies for the external client within the content that the true insecure reference was removed *before being provided to the external client."* to allow for intervention of data being delivered across secure Internet connection as suggested by Brown **[Brown: abstract: par. [0012].**

As per claim 2:

The combination of Subramaniam, Barton, and Brown teaches the subject matter as described above.

Subramaniam further teaches the method of claim 1 wherein the detecting further includes translating any non-secure links into secure links for some of the insecure transactions

before presenting results of the access attempts to the external client **[Subramaniam: Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)].**

As per claim 6:

The combination of Subramaniam, Barton, and Brown teaches the subject matter as described above.

Subramaniam further teaches the method of claim 1 wherein managing includes at least one or more of:

issuing alerts **[Subramaniam: Col. 11, lines 61-67]**, notifications **[Subramaniam: Col. 8, lines 40-57]**, or advisories to a monitoring entity or log.

As per claim 8:

Subramaniam teaches a method to manage secure communications implemented in a computer-readable medium and to execute on a proxy server, the method, comprising:

(a) detecting, by the proxy server, insecure transactions occurring during a secure session, the insecure transactions result from actions requested by an external client participating in the secure session [**Subramaniam : Col. 1, line 25 to Col. 2, line 25; Col. 6, lines 40-60; By checking the IP address which the request was made, the target server 104 determines that the request came from outside the security parameter 102**];

(b) inspecting, by the proxy server, the insecure transactions in advance of satisfying the actions requested by pre-acquiring content associated with the insecure transactions before

making available to the external client , and the insecure transactions are associated with links to an external site [[located outside a secure site associated with the secure session]], and content are pre-acquired from the external site via the links and inspected and scanned on behalf of the external client within the proxy server **[Subramaniam : Col. 1, line 25 to Col. 2, line 25; Col. 6, lines 46-60; A target server check user permissions against access control lists; fig. 1, Border server 106 includes URL transformer 108 and cache(s) 110; fig. 3; Border server 106; Col. 9, lines 32-43; "The possibly repeated acts within the transmitting step 128 involve sending one or more Web pages, files, or other pieces of non-secure data 130 from the target server 104 to the border server 106. The data 130 is non-secure in that it includes hypertext links, URLs, or other references which, if presented by the external client 112 to the secure network 100, ...which contain URLs specifying "http://" rather than "https://" in reference to data stored on the target server 104 are examples of non-secure data 130"; Col. 10, lines 10-19; Col. 5, lines 42-49; proxy servers]**; and

(c) making, by the proxy server, a determination based on the inspection for taking processing actions including one or more of the following:

(d) permitting some of the insecure transactions to proceed unmodified by performing the actions requested for the external client;

(d) permitting, by the proxy server, some of the insecure transactions to proceed in a modified fashion **[Subramaniam : Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)]** .

Subramaniam does not explicitly disclose "the border server is external from secure site, denying some of the insecure transactions by denying the actions requested, and some of the

insecure transactions that are denied are identified as references that have a World-Wide Web (WWW) cookie associated with their headers, and wherein these references are entirely removed from the content before the content is supplied to the external client and the references entirely removed are reported as custom warning to the external client as an event within the content, the event identifies for the external client within the content that the true insecure reference was removed before being provided to the external client."

It would have been obvious to one of ordinary skill in the art at the time the invention was made to move the border server to an site external from the secure location, since it has been held that it requires routine skill in the art to rearrange the location of the border server because it would not have modified the operation of the device **[See MPEP 2144.04; see also In re Japikse, 181 F.2d 1019, 86 USPQ 70 (CCPA 1950)].**

Barton discloses transferring data via a secure network connection, wherein denying some of the insecure transactions by denying the actions requested, and some of the insecure transactions that are denied are identified as references **[Barton: par. [0012]; par. [0014], the data is able to scanned for illegal content before it is delivered to the client; [0018]; par. [0033]; if illegal content is found, the this trigger an appropriate action; fig. 4, par. [0039]]**

Barton further disclose a https proxy computer scanning for illegal content and triggering an appropriate action such as sending a warning webpage to client or issue of an alert to a network administrator **[Barton: figs 4-5; par. [0033], [0039], [0040]].**

Therefore, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Barton with the teaching of

Subramaniam to ensure that a transferring data does not contain any illegal content by scanning for illegal content before data is delivered to a client **[Barton: par. [0014]].**

Subramaniam and Barton do not explicitly disclose *"World*-Wide Web (WWW) cookie associated with their headers, and these references are entirely removed from the content before the content is supplied to the external client and the references entirely removed are reported as custom warning messages to the external client as and an event identifies for external client within a content, the event identifies for the external client within the content that the true *insecure reference was removed before being provided to the external client"* Instead, Barton disclose a content that is scanned identifies a true insecure reference by determining that the true insecure reference is a particular reference that has been determined by the method to have had the piece of the content or metadata of the true insecure reference tampered with **[Barton: par. [0012]; scanning code operable to scan said data at said proxy computer for illegal content (i.e. a true insecure reference); See also par. [0014], [0018]; par. [0033]; if illegal content is found (i.e. a true insecure reference has been tampered), then this trigger an appropriate action; fig. 4, par. [0039];** Barton further discloses a https proxy computer scanning for illegal content and triggering an appropriate action such as sending a warning webpage to client or issue of an alert to a network administrator **[Barton: figs 4-5; par. [0033], [0039], [0040]].**

However, in the same field of art, Brown teaches system and method for transcoding support of Web content over secure connection. In at least one of embodiment, Brown teaches step of executing an URL request with a modified request header, removing a set-cookie directive from header, and sending modified http response to a client [**Brown: fig. 4, par. [0032-**

0041]; modified a request header' removed a set-cookie directive from http response. Set-cookie directives are not sent to client; Send modified http response to client].

Therefore, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Brown with the teaching of Subramaniam and Barton invention, by implementing "World-Wide Web (WWW) cookie associated with their headers, and wherein these references are entirely removed from the content before the content is supplied to the external client and the references entirely removed are reported as custom warning messages to the external client as an event within the content, the event identifies for the external client within the content that the true insecure reference was *removed before being provided to the external client."* to allow for intervention of data being delivered across secure Internet connection as suggested by Brown **[Brown: abstract: par. [0012].**

As per claim 13:

Subramaniam further discloses the method of claim 8 wherein the making a determination further includes permitting some of the insecure transactions to proceed in a modified fashion by transparently processing the external client access attempt within the proxy server making the external client access attempt appear to be part of the secure session **[Subramaniam: Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)].**

Claims 10, 12, and 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Number 6,081,900 (hereinafter **Subramaniam**) in view of US Patent Application Publication US 2003/0131259 A1 (hereinafter **Barton**) further in view US Patent Application Publication 2003/0061387 A1 (hereinafter **Brown**), and further in view of "Netscape Proxy Server Administrator's Guide Version 3.5 for Unix", 1997, as provided by applicant (hereinafter **Netscape_unix_v3.5**)

As per claim 10:

The combination of Subramaniam, Barton, and Brown teaches the subject matter as described above.

Subramaniam further discloses a method permitting the insecure transactions to proceed in the modified fashion by changing the reference links from Hypertext Transfer Protocol (HTTP) insecure links to HTTP over Secure Sockets Layer (HTTPS) **[Subramaniam : Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)].**

The combination of Subramaniam, Barton, and Brown do not explicitly disclose to suppress security warning messages.

However, Netscape_unix_v3.5 discloses to suppress security warning messages **[Netscape_unix_v3.5: Chapter 10, pages 1-3; A proxy server can be configured a custom message, which sends to an external client. A customized text message can be an empty text].**

Thus, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Subramaniam, Barton, and Brown by including the teaching of Netscape_unix_v3.5 because it would improve warning techniques for managing secure warning communications by triggering appropriate action such as sending of a warning webpage to client or an issue of an alert message to a network administrator **[Barton: par. [0033]].**

As per claim 12:

The combination of Subramaniam, Barton, and Brown teaches the subject matter as described above.

Subramaniam discloses a method permitting insecure transactions to proceed unmodified **[Subramaniam: Col. 2, lines 36-41].**

Subramaniam, Barton, and Brown do not explicitly disclose permitting normally occurring security warnings to be presented to the client before satisfying the external client access attempt to reference the external site.

However, Netscape_unix_v3.5 discloses permitting normally occurring security warnings to be presented to external the client before satisfying the external client access attempt to reference the external site **[Netscape_unix_v3.5 : Chapter 10, pages 1-3; Chapter 13, page 1; A proxy server can be configured a custom message, which sends to an external client. A customized text message can be security warning messages].**

Thus, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Subramaniam, Barton, and Brown by including

the teaching of Netscape_unix_v3.5 because it would improve warning techniques for managing secure warning communications by triggering appropriate action such as sending of a warning webpage to client or an issue of an alert message to a network administrator **[Barton: par. [0033]].**

As per claim 14:

The combination of Subramaniam, Barton, and Brown teaches the subject matter as described above.

Subramaniam, Barton, and Brown do not explicitly disclose method, wherein the making a determination further includes denying the insecure transactions after determining that the external client access attempt is corrupted and notifying the external client of a denial.

However, Netscape_unix_v3.5 discloses a method wherein the making a determination further includes denying the insecure transactions after determining that the external client access attempt is corrupted and notifying the external client of a denial **[Netscape_unix_v3.5: Chapter 13, page 1; A proxy will issue a fatal error (i.e. catastrophe) if an outside agent causes cache files to become corrupt].**

Thus, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Subramaniam, Barton, and Brown by including the teaching of Netscape_unix_v3.5 because it would improve warning techniques for managing secure warning communications by triggering appropriate action such as sending of a warning webpage to client or an issue of an alert message to a network administrator **[Barton: par. [0033]].**

As per claim 15:

The combination of Subramaniam, Barton, and Brown teaches the subject matter as described above.

Subramaniam, Barton, and Brown do not explicitly disclose the method of claim 8 wherein the making a determination further includes denying the some of the insecure transactions after determining that the external client access attempt is corrupted and logging information about the external client access attempt.

However, Netscape_unix_v3.5 discloses a method wherein the making a determination further includes denying the insecure transactions after determining that the external client access attempt is corrupted and logging information about the external client access attempt **[Netscape_unix_v3.5 : Chapter 13, pages 1-7].**

Thus, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Subramaniam, Barton, and Brown by including the teaching of Netscape_unix_v3.5 because it would improve warning techniques for managing secure warning communications by triggering appropriate action such as sending of a warning webpage to client or an issue of an alert message to a network administrator **[Barton: par. [0033]].**

Conclusion

The Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the Applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the Applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

The Examiner requests, in response to this Office action, support be shown for language added to any original claims on amendment and any new claims. That is, indicate support for newly added claim language by specifically pointing to page(s) and line number(s) in the specification and/or drawing figure(s). This will assist the examiner in prosecuting the application. Failure to show support can result in a non-compliant response.

When responding to this office action, Applicant is advised that if Applicant traverses an obviousness rejection under 35 U.S.C. 103, a reasoned statement must be included explaining why the Applicant believes the Office has erred substantively as to the factual findings or the conclusion of obviousness See 37 CFR 1.111(b).

Additionally Applicant is further advised to clearly point out the patentable novelty which he or she thinks the claims present, in view of the state of the art disclosed by the references cited or the objections made. He or she must also show how the amendments avoid such references or objections See 37 CFR 1.111(c).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Orgad Edan can be reached on 571-272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Canh Le/

Examiner, Art Unit 2439

March 12, 2011

/Christopher J Brown/

Primary Examiner, Art Unit 2439